04-03-00 A

Please type a plus sign (+) inside this box → +

PTO/SB/05 (4/98)
Approved for use through 09/30/2000. OMB 0651-0032
Patent and Trademark Office. U.S DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1 53(b))

Attorney Docket No.	042390.P8083
First Inventor or Application Identifier	David W. Grawrock
Title	PROTECTION OF A ROOT CERTIFIER IN HARDWARE
Express Mail Label No.	EL466333693US

jc688 U.S. PTO 02/31/00

jc530 U.S. PTO 09/540614 03/31/00

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. ☒ Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)

2. ☒ Specification [Total Pages 16]
(preferred arrangement set forth below)
- Descriptive title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings (*if filed*)
- Detailed Description
- Claim(s)
- Abstract of the Disclosure

3. ☒ Drawing(s) *(35 U.S.C. 113)* [Total Sheets 2]

4. Oath or Declaration [Total Pages 3]
a. ☐ Newly executed (original copy)
b. ☐ Copy from a prior application (37 C.F.R. § 1.63(d)) *(for continuation/divisional with Box 16 completed)*
i. ☐ DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR §§ 1.63(d)(2) and 1.33(b).

5. ☐ Microfiche Computer Program *(Appendix)*

6. Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all necessary)*
a. ☐ Computer Readable Copy
b. ☐ Paper Copy (identical to computer copy)
c. ☐ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

7. ☐ Assignment Papers (cover sheet & document(s))
8. ☐ 37 C.F.R. § 3.73(b) Statement *(when there is an assignee)* ☐ Power of Attorney
9. ☐ English Translation Document *(if applicable)*
10. ☐ Information Disclosure Statement (IDS)/PTO - 1449 ☐ Copies of IDS Citations
11. ☐ Preliminary Amendment
12. ☐ Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
13. ☐ *Small Entity Statement(s) ☐ Statement filed in prior application, Status still proper and desired
14. ☐ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
15. ☐ Other: .....

NOTE FOR ITEMS 1 & 13: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).

16. **If a CONTINUING APPLICATION**, *check appropriate box, and supply the requisite information below and in a preliminary amendment:*
☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No: _____

Prior application Information: Examiner _____ *Group/Art Unit:* _____

For CONTINUATION or DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts

17. CORRESPONDENCE ADDRESS

☐ *Customer Number of Bar Code Label* (Insert Customer No. or Attach bar code label here) or ☒ *Correspondence address below*

Name	BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP				
Address	12400 Wilshire Boulevard, Seventh Floor				
City	Los Angeles	State	California	Zip Code	90025
Country	U.S.A.	Telephone	(714) 557-3800	Fax	(714) 557-3347

Name (Print/Type)	William W. Schaal, Reg. No. 39,018		
Signature		Date	03/31/00

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231 DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231

Atty. Docket No.: 042390.P8084
Express Mail No.: EL466333680US

APPLICATION FOR UNITED STATES PATENT

FOR

A DEVICE AND METHOD FOR DISABLING AN OVERRIDE HARDWARE PIN ASSERTION

Attorney Docket No. 042390.P8084

Inventor(s):

DAVID W. GRAWROCK

Prepared by:

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
12400 Wilshire Boulevard, Seventh Floor
Los Angeles, California 90025-1026
(714) 557-3800

BACKGROUND

1. Field

This invention relates to the field of data security. In particular, the invention relates to an apparatus and method for protecting confidential information stored within an electronic system.

2. Background

Advances in technology have opened up many opportunities for applications that go beyond the traditional ways of doing business. Electronic commerce (e-commerce) and business-to-business (B2B) transactions are now becoming popular, reaching the global markets at a fast rate. Unfortunately, while electronic systems like computers provide users convenient and efficient methods of doing business, communicating and transacting, they are also vulnerable for unscrupulous attacks. Examples of these attacks include virus, intrusion, exposure of private information, and tampering, to name a few. Therefore, it is becoming more and more important to protect the integrity of the contents of a computer, primarily to maintain user confidence in computer based transactions.

Recently, some Intel® Architecture computers are being employed with a firmware hub. To reduce the risk of unauthorized tampering with the stored contents of the firmware hub, control application software can be installed within the computer. The control application software is designed to preclude the deletion of data stored within flash memory of the firmware hub unless this software detects that the user correctly entered a previously negotiated pass phrase.

In the event that the pass phrase is forgotten by the user, the firmware hub includes an override pin which, when asserted, signals the control application software to

ignore the current pass phrase and enable a new pass phrase to be created. In certain situations, however, the override pin can be misused. For example, security features of a stolen computer can be deleted from the flash memory of the firmware hub after assertion of the override pin and entering of a new pass phrase selected by the thief.

There exists a need to temporarily disable the override pin to provide users of electronic systems with an ability to eliminate this recognized breach of system security.

Express Mail No. EL466333680US

BRIEF DESCRIPTION OF THE DRAWINGS

The features and advantages of the present invention will become apparent from the following detailed description of the present invention in which:

Figure 1 is an exemplary block diagram of an embodiment of a product employing an electronic system practicing the invention.

Figure 2 is an exemplary block diagram of an embodiment of the electronic system including a packaged IC device having an override disabled pin.

Figure 3 is an exemplary block diagram of the IC device of Figure 2.

Figure 4 is an exemplary block diagram of the pin configuration of the package of the IC device.

Figure 5 is an exemplary flowchart of the operations of the packaged IC device.

PCT/US2003/000000

DESCRIPTION

The present invention relates to an apparatus and method for protecting information stored within an electronic system. More specifically, the invention comprises the addition of an override disable pin to the packaging architecture of an integrated circuit device such as the firmware hub for example. When asserted, the override disable pin sets a non-volatile bit storage element within the integrated circuit device. In the event that the override pin of the integrated circuit device is asserted, control application software running on the electronic system checks whether the non-volatile bit storage element is set and if so, denies the user access to information stored within the integrated circuit device unless a previously negotiated pass phrase is entered.

Herein, certain details are set forth in order to provide a thorough understanding of the present invention. It is apparent to a person of ordinary skill in the art, however, that the present invention may be practiced through many embodiments other that those illustrated. Well-known circuits are not set forth in detail in order to avoid unnecessarily obscuring the present invention.

In the following description, terminology is used to discuss certain features of the present invention. For example, an "electronic system" includes any product that requires user authentication before providing access to its stored content. Examples of an electronic system include, but are not limited or restricted to a computer (e.g., desktop, a laptop, a server, a workstation, a hand-held, etc.), desktop office equipment (e.g., photocopier, printer, scanner, etc.), a television set-top box, and the like. A "link" is broadly defined as one or more information-carrying mediums (e.g., electrical wire, optical fiber, cable, bus, etc.) or wireless communications through infrared, radio frequency (RF) signaling, or any other wireless signaling mechanism.

In addition, the term "information" is defined as one or more bits of data, address, and/or control. A "pass-phrase" is a series of bits originating from a string of inputted alphanumeric characters, voice patterns and the like. In the context of information, the term "modify" (and related tenses) involves an act of either (i) adding, or (ii) deleting, or (iii) overwriting information. A "cryptographic operation" is an operation performed for additional data security such encryption, decryption, performing computations involving a digital signature, performing computations involving a digital certificate, and the like.

Referring to Figure 1, a perspective view of an illustrative embodiment of a product employing the present invention is shown. The product 100 comprises an electronic system 110 for processing data and a monitor 120 for displaying such data. The monitor 120 may include a flat panel display (e.g., liquid crystal display, active matrix display, etc.), a cathode ray tube, or any other type of display technology. The electronic system 110 further includes a receiver 130 to receive information over a link 140 and/or a transmitter 135 to transmit information over the link 140. For example, the receiver/transmitter 130/135 may include a modem that is situated external to a chassis 150 of the product 100 (as shown) or internal circuitry (e.g., a modem card, networking card, etc.) placed within the chassis 150.

Referring still to Figure 1, for this embodiment, the electronic system 110 receives as input information from one or more user input devices 160. The user input device 160 may be integrated within or physically remote from the chassis 150. Examples of a user input device 160 include, but are not restricted or limited to a keyboard, a keypad, a trackball, a mouse, a stylus, a microphone and the like.

Referring now to Figure 2, an illustrative block diagram of an embodiment of an electronic system 110 is shown. Electronic system 110 includes a processor 200, a memory control hub (MCH) 210, a system memory 220, an input/output control hub (ICH) 230, and a packaged integrated circuit (IC) device 240 (e.g., a firmware hub) which

supports communications with at least one of the user input devices 160 of Figure 1. The packaged IC device 240 features protected non-volatile memory memory and cryptographic logic as described in Figure 3.

In general, the packaged IC device 240 operates in a plurality of modes. For example, the packaged IC device 240 may be placed in an administrator mode when the user issues a request to alter the functionality of the electronic system 110. This is accomplished by controlling access to entering the administrator mode, possible through modification of its stored contents. Otherwise, the packaged IC device 240 operates in a user mode. For example, when performing cryptographic operation, like digitally signing information or encrypting/decrypting information, for example, the IC device 240 is in user mode.

As shown in Figure 2, the processor 200 represents a central processing unit of any type of architecture, such as complex instruction set computers (CISC), reduced instruction set computers (RISC), very long instruction word (VLIW), or hybrid architecture. In one embodiment, the processor 200 is compatible with the Intel® Architecture (IA) processor, such as the IA-32 and the IA-64. Of course, in an alternative embodiment, the processor 200 may include multiple processing units coupled together over a common host bus 205.

Coupled to the processor 200 via the host bus 205, the MCH 210 may be integrated into a chipset that provides control and configuration of memory and input/output devices such as the system memory 220 and the ICH 230. The system memory 220 stores system code and data. The system memory 220 is typically implemented with dynamic random access memory (DRAM) or static random access memory (SRAM). It is contemplated, however, that the system memory 220 may be segmented into an accessible physical memory area 221 and an isolated memory area 222. Access to contents within the isolated memory area 222 is restricted and enforced

by the processor 200 and/or the MCH 210 or other chipset that integrates the isolated area functionalities. The system memory 220 may also include other programs or data that are not shown.

The ICH 230 may also be integrated into a chipset together or separate from the MCH 210 to perform I/O functions. As shown, the ICH 230 enables communications to the packaged IC device 240 via link 250 from one or more user input devices 160 (e.g., a keyboard, keypad, etc.). Also, the ICH 230 enables communications to devices coupled to other links such as a Peripheral Component Interconnect (PCI) bus at any selected frequency (e.g., 66 megahertz "MHz", 100 MHz, etc.), an Industry Standard Architecture (ISA) bus, a Universal Serial Bus or another bus configured with a different architecture than those briefly mentioned.

Referring to Figure 3, an illustrative block diagram of the packaged IC device 240 is shown. The packaged IC device 240 comprises one or more integrated circuits placed within a protective IC package 300. For clarity sake, the packaged IC device 240 is based on an integrated circuit that comprises (i) logic 310 to perform a cryptographic operation, (ii) a non-volatile memory 315 (e.g., flash memory), and (iii) one or more control storage elements 330.

In particular, one portion of the non-volatile memory 315 is loaded with a representation 316 of the primary pass-phrase such as a hash value (result after the pass-phrase undergoes a one-way hash function) or any other computed value. Of course, the representation 316 could be the primary pass-phrase in its entirety.

Another portion of the non-volatile memory 315 includes microcode 317 that communicates with control application software executed by the processor 200 and accessible by the user. When the user desires to modify stored contents of the non-volatile memory, the control application software sends a message to the microcode 317

to determine whether or not access is granted or denied. One parameter of the message includes a previously negotiated, primary pass-phrase; however, other parameters of the message are based on the chosen Application Programming Interface (API) 318 between the microcode 317 and the control application software.

Another portion 319 of the non-volatile memory 315 is segregated into a plurality "N" of protected storage areas 320_1-320_N ($N \geq 1$), each having a predetermined size (referred to as "slots"). Each slot 320_1-320_N features an access control mechanism (ACM) 325_1-325_N that determines whether the user has access to the particular slot $320_1,\ldots, 320_N$. For example, access control mechanism 325_1 determines whether a secondary pass-phrase, provided by the user, indicates that user has access to the contents of the slot 320_1.

As further shown in Figure 3, the control storage element(s) 330 of the packaged IC device 240 is set upon assertion of an override disable pin 350. In one embodiment, the control storage element 330 includes one or more control registers configured for permanent state retention, namely maintaining its bit state through any number of power cycles. The control storage element 330 can be cleared only by providing the correct primary pass-phrase to place the packaged IC device into an administrator mode and clearing the state of the storage element 330 thereafter.

As shown in Figure 4, package 300 may include a 32-pin package featuring an override pin 340 and an override disable (OD) pin 350, although any size package may be used provided its pin configuration supports override and override disable signaling. In general, the assertion of the override pin 340 signals the control application software 225 to ignore the current, primary pass-phrase and allows the user to modify the primary pass-phrase. The assertion of the override disable pin 350 effectively signals the control application software running on the electronic system 110 to ignore the assertion of the

override pin 310 and still requires entry of the correct primary pass-phrase to gain access to stored content of the integrated circuit(s).

Referring now to Figure 5, a flowchart of the operations for disabling an override hardware pin assertion for the electronic system is shown. First, the user places the IC device into an administrator mode. For example, this may accomplished by the user selecting a control panel, which causes a window to be generated. The user enters a primary pass-phrase within a selected field of the window and selects an ENTER button on the window. The primary pass-phrase undergoes a computation (e.g., a one-way hash function) to produce a representation (e.g., hash value) and one or more parameters, inclusive of the representation, is transferred through the API to the microcode (blocks 500 and 510). The microcode compares the incoming representation with a prestored representation such as comparing the incoming hash value with a prestored hash value (block 520). If the primary pass-phrase is correct, the IC device is placed in the administrator mode (block 530). Otherwise, the IC device remains in its user mode.

During the administrator mode, the primary pass-phrase may be modified, the contents of the control storage element may be modified, or the contents of the slots within the non-volatile memory of the IC device may be deleted. However, if it is desirable to modify the contents of the first slot for example, the user is required to enter a secondary pass-phrase. Similarly, as described above, the input secondary pass-phrase undergoes a hash function to produce a hash value that is compared with a hash value prestored by the microcode. This prestored hash value associated with the first slot is contained in the storage area associated with the access control mechanism of the first slot. If the secondary pass-phrase is correct, the contents may be altered. Otherwise, the contents are not modifiable, but can be deleted and restored.

If the user fails to remember his or her primary pass-phrase, the override pin of the IC device may be asserted (block 540). If the override disable pin has not been

previously asserted so that the control storage element is set, the user may reconfigure the electronic system with a new primary pass-phrase (blocks 550 and 560). Upon selection, a representation (e.g., hash value) of the new primary pass-phrase is loaded into the non-volatile memory of the IC device (block 570). However, if the control storage element is set, the IC device signals the control application software that the user may not gain access to the stored content of the IC device unless the correct primary pass-phrase is entered (blocks 550 and 580).

In summary, in the normal case, when the override disable pin is not set, a system of the override pin allows the user to reset the primary pass-phrase and give access to the administrator mode. However, when the override disable pin is set, access to the administrator mode is restricted to only those parties who recall the primary pass-phrase.

While this invention has been described with reference to illustrative embodiments, this description is not intended to be construed in a limiting sense. Various modifications of the illustrative embodiments, as well as other embodiments of the invention, which are apparent to persons skilled in the art to which the invention pertains are deemed to lie within the spirit and scope of the invention.

What is claimed is:

1. A method comprising:

implementing an integrated circuit device within an electronic system, the integrated circuit device including an override disable pin; and

preventing modification of a representation of a primary pass-phrase when the override disable pin is asserted, the primary pass-phrase permitting access to stored information within the electronic system.

2. The method of claim 1, wherein the integrated circuit device comprises a package to form a packaged integrated circuit device.

3. The method of claim 1, wherein preventing of the modification of the primary pass-phrase includes

setting a control storage element within the integrated circuit device upon assertion of the override disable pin; and

disabling modification of the primary pass-phrase when the control storage element is set.

4. The method of claim 3, wherein the control storage element is set after placing the electronic system in an administration mode upon correctly inputting the primary pass-phase into the electronic system.

5. The method of claim 1, wherein the integrated circuit device further includes an override pin which, when asserted, allows a stored representation of the primary pass-phrase to be modified.

6. The method of claim 1, wherein the preventing of the modification of the primary pass-phrase includes signaling a control application software initiating a request for modification of the pass-phrase that a user is denied access to the stored information of the integrated circuit device unless the primary pass-phrase is correctly entered.

7. The method of claim 1, wherein the representation of the primary pass-phrase includes a hash value of the primary pass-phrase.

8. The method of claim 1, wherein control storage element includes at least one control register configured for permanent state retention over a plurality of power cycles.

9. A method comprising:

enabling access to stored information within an electronic system upon assertion of an override disable pin of an integrated circuit device; and

disabling access to the stored information despite assertion of the override pin of the integrated circuit device when an override disable pin of the integrated circuit device is asserted prior to assertion of the override pin.

10. The method of claim 9, wherein the integrated circuit device comprises a package to form a packaged integrated circuit device.

11. The method of claim 9, wherein the act of disabling access comprises

setting a control storage element within the integrated circuit device in response to the assertion of the override disable pin; and

determining whether the control storage element is set.

12. The method of claim 11, wherein the control storage element is set after placing the electronic system in an administration mode upon correctly inputting the primary pass-phase into the electronic system.

13. The method of claim 9, wherein the setting of the control storage element includes setting a bit of at least one control register configured for permanent state retention over a plurality of power cycles.

14. A method comprising:

enabling placement of an electronic system into an administrator mode upon assertion of an override disable pin of an integrated circuit device; and

disabling placement of the electronic system into the administrator mode despite assertion of the override pin of the integrated circuit device when an override disable pin of the integrated circuit device is asserted prior to assertion of the override pin.

15. The method of claim 14, wherein the integrated circuit device comprises a package to form a packaged integrated circuit device.

16. The method of claim 14, wherein the act of disabling access comprises

setting a control storage element within the integrated circuit device in response to the assertion of the override disable pin; and

determining whether the control storage element is set.

17. The method of claim 14, wherein the setting of the control storage element includes setting a bit of at least one control register configured for permanent state retention over a plurality of power cycles.

18. An electronic system comprising:

a bus;

a processor coupled to the bus;

a system memory coupled to the bus; and

an integrated circuit device coupled to the bus, the integrated circuit device including:

a memory,

an override pin to enable access to information stored within the memory upon assertion of the override pin, and

an override disable pin to disable access to the information stored within the memory despite the assertion of the override pin when the override disable pin is asserted prior to assertion of the override pin.

19. The electronic system of claim 18, wherein the integrated circuit further comprises a package to contain the memory from which the override pin and the override disable pin protrude.

20. The electronic system of claim 18, wherein the memory of the integrated circuit device is non-volatile memory.

21. The electronic system of claim 18, wherein the integrated circuit device further includes a control storage element.

22. The electronic system of claim 21, wherein the control storage element of the integrated circuit device includes at least one control register configured for permanent state retention over a plurality of power cycles.

23. The electronic system of claim 18, wherein the integrated circuit device further includes a microcode to determine whether the override disable pin has been asserted prior to assertion of the override pin.

Attorney Docket No. 042390.P8084

ABSTRACT

One embodiment of present invention is a method for preventing the modification of a primary pass-phrase of an electronic system. Access to stored information such as a primary pass-phrase is disabled despite assertion of an override pin of an integrated circuit device of the electronic device when an override disable pin of the integrated circuit device is asserted prior to assertion of the override pin.

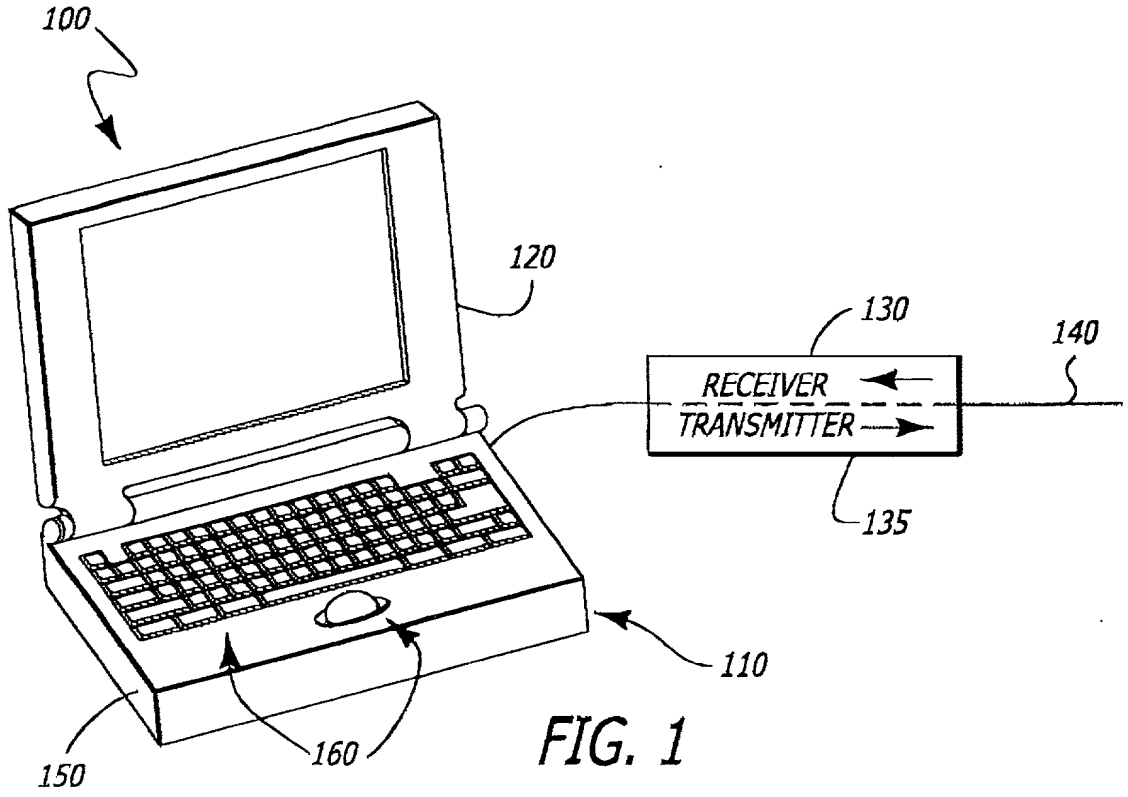
100
120
130
140
RECEIVER
TRANSMITTER
135
110
150
160

FIG. 1

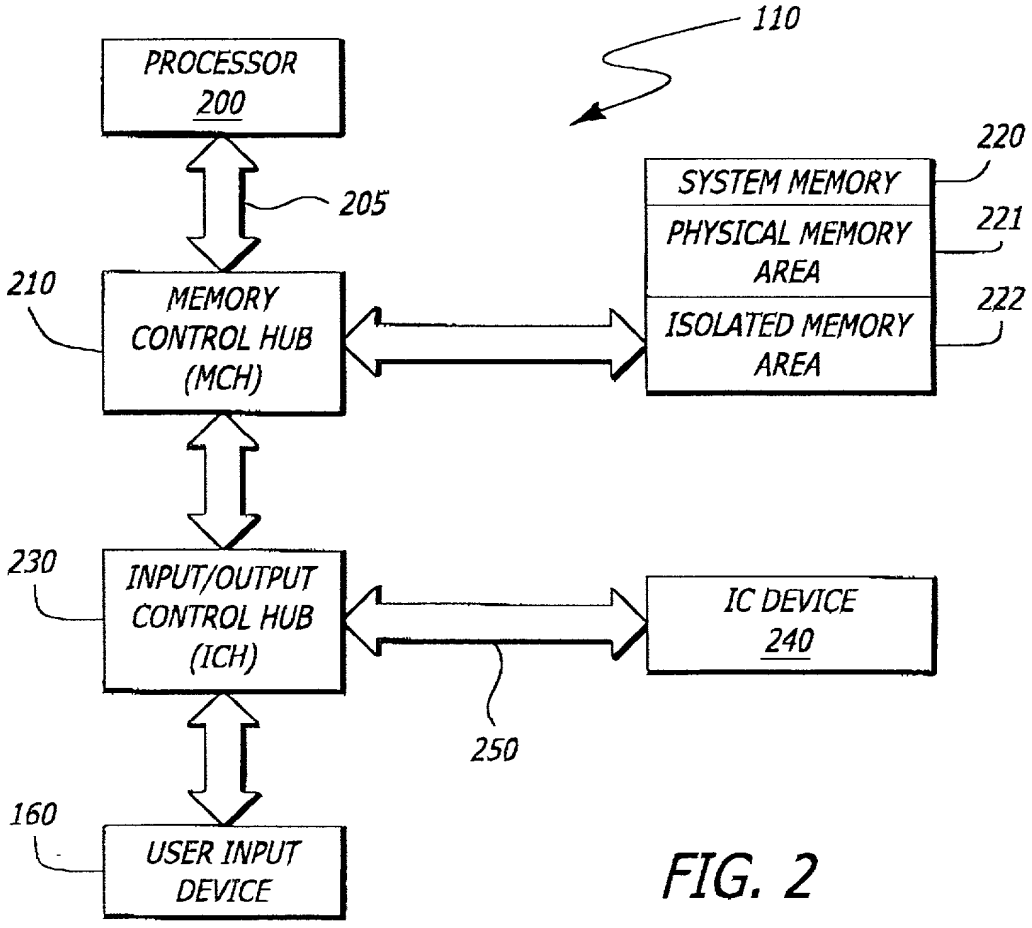
110
PROCESSOR
200
205
220
SYSTEM MEMORY
PHYSICAL MEMORY AREA
221
222
ISOLATED MEMORY AREA
210
MEMORY CONTROL HUB (MCH)
230
INPUT/OUTPUT CONTROL HUB (ICH)
IC DEVICE
240
250
160
USER INPUT DEVICE

FIG. 2

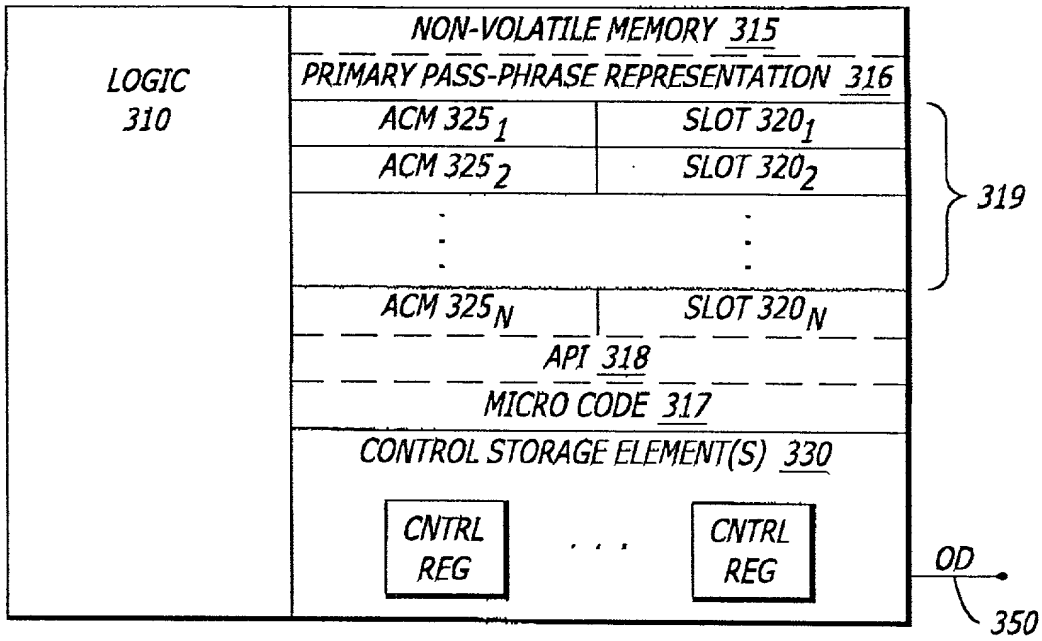
LOGIC
310
NON-VOLATILE MEMORY 315
PRIMARY PASS-PHRASE REPRESENTATION 316
ACM 325 1
SLOT 320 1
ACM 325 2
SLOT 320 2
319
ACM 325 N
SLOT 320 N
API 318
MICRO CODE 317
CONTROL STORAGE ELEMENT(S) 330
CNTRL REG
CNTRL REG
OD
350

FIG. 3

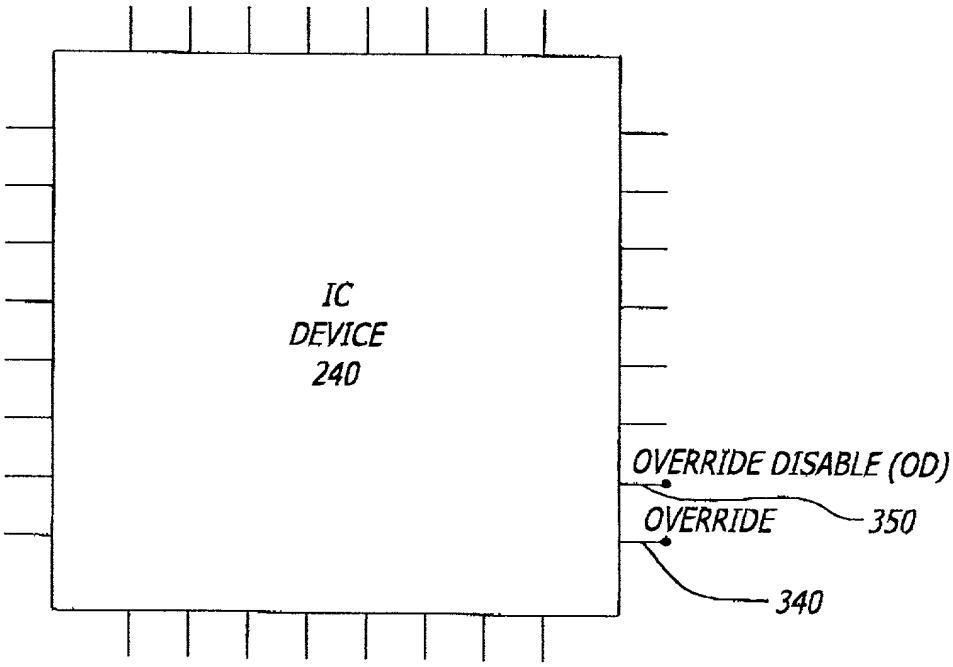
IC
DEVICE
240
OVERRIDE DISABLE (OD)
350
OVERRIDE
340

FIG. 4

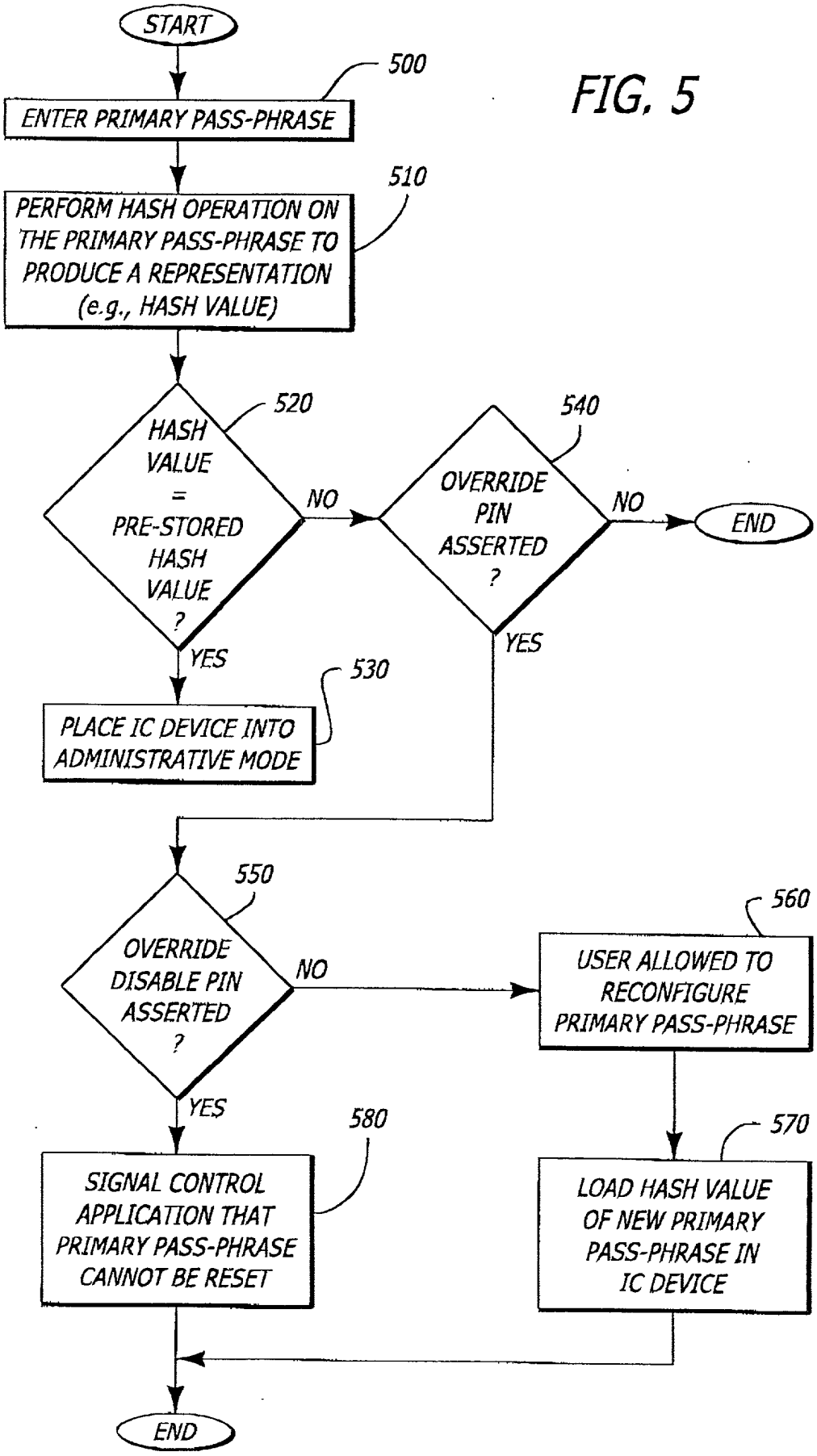
START
500
ENTER PRIMARY PASS-PHRASE
510
PERFORM HASH OPERATION ON THE PRIMARY PASS-PHRASE TO PRODUCE A REPRESENTATION (e.g., HASH VALUE)
520
HASH VALUE = PRE-STORED HASH VALUE ?
NO
540
OVERRIDE PIN ASSERTED ?
NO
END
YES
YES
530
PLACE IC DEVICE INTO ADMINISTRATIVE MODE
550
OVERRIDE DISABLE PIN ASSERTED ?
NO
560
USER ALLOWED TO RECONFIGURE PRIMARY PASS-PHRASE
YES
580
SIGNAL CONTROL APPLICATION THAT PRIMARY PASS-PHRASE CANNOT BE RESET
570
LOAD HASH VALUE OF NEW PRIMARY PASS-PHRASE IN IC DEVICE
END

FIG. 5

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION (FOR INTEL CORPORATION PATENT APPLICATIONS)

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name.

I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

A DEVICE AND METHOD FOR DISABLING AN OVERRIDE HARDWARE PIN ASSERTION

the specification of which

[X] is attached hereto.

[ ] was filed on _____ as
United States Application Number _____
or PCT International Application Number _____
and was amended on _____.
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s):

APPLICATION NUMBER	COUNTRY (OR INDICATE IF PCT)	DATE OF FILING (day, **month**, year)	PRIORITY CLAIMED UNDER 37 USC 119
			☐ No ☐ Yes
			☐ No ☐ Yes
			☐ No ☐ Yes

I hereby claim the benefit under Title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below:

APPLICATION NUMBER	FILING DATE

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

APPLICATION NUMBER	FILING DATE	STATUS (ISSUED, PENDING, ABANDONED)

I hereby appoint the persons listed on Appendix A hereto (which is incorporated by reference and a part of this document) as my respective patent attorneys and patent agents, with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to:
William W. Schaal, Reg. No. 39,018, BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP
(Name of Attorney or Agent)
12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025 and direct telephone calls to:
William W. Schaal, (714) 557-3800.
(Name of Attorney or Agent)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor (given name, family name) **David W. Grawrock**

Inventor's Signature _____ Date _____

Residence Aloha, Oregon USA Citizenship USA
(City , State) *(Country)*

P. O. Address 8285 SW 184th Avenue

Aloha, Oregon 97007 USA

APPENDIX A

I hereby appoint BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, a firm including: William E. Alford, Reg. No. 37,764; Farzad E. Amini, Reg. No. 42,261; Amy M. Armstrong, Reg. No. 42,265; Aloysius T. C. AuYeung, Reg. No. 35,432; William Thomas Babbitt, Reg. No. 39,591; Carol F. Barry, Reg. No. 41,600; Jordan Michael Becker, Reg. No. 39,602; Bradley J. Bereznak, Reg. No. 33,474; Michael A. Bernadicou, Reg. No. 35,934; Roger W. Blakely, Jr., Reg. No. 25,831; Gregory D. Caldwell, Reg. No. 39,926; Ronald C. Card, Reg. No. 44,587; Thomas M. Coester, Reg. No. 39,637; Donna Jo Coningsby, Reg. No. 41,684; Michael Anthony DeSanctis, Reg. No. 39,957; Daniel M. De Vos, Reg. No. 37,813; Robert Andrew Diehl, Reg. No. 40,992; Matthew C. Fagan, Reg. No. 37,542; Tarek N. Fahmi, Reg. No. 41,402; George L. Fountain, Reg. No. 36,374; Paramita Ghosh, Reg. No. 42,806; James Y. Go, Reg. No. 40,621; James A. Henry, Reg. No. 41,064; Willmore F. Holbrow III, Reg. No. 41,845; Sheryl Sue Holloway, Reg. No. 37,850; George W Hoover II, Reg. No. 32,992; Eric S. Hyman, Reg. No. 30,139; William W. Kidd, Reg. No. 31,772; Sang Hui Kim, Reg. No. 40,450; Eric T. King, Reg. No. 44,188; Erica W. Kuo, Reg. No. 42,775; Michael J. Mallie, Reg. No. 36,591; Paul A. Mendonsa, Reg. No. 42,879; Darren J. Milliken, Reg. No. 42,004; Chun M. Ng, Reg. No. 36878; Thien T. Nguyen, Reg. No. 43,835; Thinh V. Nguyen, Reg. No. 42,034; Dennis A. Nicholls, Reg. No. 42,036; Lisa A. Norris, Reg. No. 44,976; Daniel E. Ovanezian, Reg. No. 41,236; William F. Ryann, Reg. No. 44,313; James H. Salter, Reg. No. 35,668; William W. Schaal, Reg. No. 39,018; James C. Scheller, Reg. No. 31,195; Jeffrey S. Smith, Reg. No. 39,377; Maria McCormack Sobrino, Reg. No. 31,639; Stanley W. Sokoloff, Reg. No. 25,128; Judith A. Szepesi, Reg. No. 39,393; Vincent P. Tassinari, Reg. No. 42,179; Edwin H. Taylor, Reg. No. 25,129; Joseph A. Twarowski, Reg. No. 42,191; Lester J. Vincent, Reg. No. 31,460; Glenn E. Von Tersch, Reg. No. 41,364; John Patrick Ward, Reg. No. 40,216; Charles T. J. Weigell, Reg. No. 43,398; James M. Wu, Reg. No. 45,241; Steven D. Yates, Reg. No. 42,242; and Norman Zafman, Reg. No. 26,250; my attorneys; and Andrew C. Chen, Reg. No. 43,544; Justin M. Dillon, Reg. No. 42,486; and John F. Travis, Reg. No. 43,203; my patent agents, of BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, with offices located at 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025, telephone (714) 557-3800, and Alan K. Aldous, Reg. No. 31,905; Robert D. Anderson, Reg. No. 33,826; Joseph R. Bond, Reg. No. 36,458; Richard C. Calderwood, Reg. No. 35,468; Jeffrey S. Draeger, Reg. No. 41,000; Cynthia Thomas Faatz, Reg No. 39,973; Sean Fitzgerald, Reg. No. 32,027; John N. Greaves, Reg. No. 40,362; Seth Z. Kalson, Reg. No. 40,670; David J. Kaplan, Reg. No. 41,105; Charles A. Mirho, Reg. No. 41,199; Leo V. Novakoski, Reg. No. 37,198; Naomi Obinata, Reg. No. 39,320; Thomas C. Reynolds, Reg. No. 32,488; Kenneth M. Seddon, Reg. No. 43,105; Mark Seeley, Reg. No. 32,299; Steven P. Skabrat, Reg. No. 36,279; Howard A. Skaist, Reg. No. 36,008; Steven C. Stewart, Reg. No. 33,555; Raymond J. Werner, Reg. No. 34,752; Robert G. Winkle, Reg. No. 37,474; and Charles K. Young, Reg. No. 39,435; my patent attorneys, and Thomas Raleigh Lane, Reg. No. 42,781; Calvin E. Wells; Reg. No. P43,256, Peter Lam, Reg. No. 44,855; and Gene I. Su, Reg. No. 45,140; my patent agents, of INTEL CORPORATION; and James R. Thein, Reg. No. 31,710, my patent attorney; with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.